**UNITED STATES DISTRICT COURT**
**WESTERN DISTRICT OF TEXAS**
**SAN ANTONIO DIVISION**

| | |
|---|---|
| DAISY TRUJILLO, individually and on behalf of all others similarly situated,<br><br>Plaintiff,<br><br>v.<br><br>NEC NETWORKS, LLC D/B/A CAPTURERX, and RITE AID CORP.<br><br>Defendants. | Case No. 5:21-cv-00523<br><br>**CLASS ACTION COMPLAINT**<br><br>**JURY TRIAL DEMANDED** |

Plaintiff Daisy Trujillo ("Plaintiff"), individually and on behalf of all others similarly situated ("Class Members"), brings this Class Action Complaint against NEC Networks, LLC d/b/a CaptureRx ("CaptureRx") and Rite Aid Corporation ("Rite Aid") (collectively, "Defendants"), and alleges, upon personal knowledge as to her own actions and the investigation of her counsel, and upon information and belief as to all other matters, as follows:

## INTRODUCTION

1. Plaintiff brings this class action against Defendants for their failure to adequately secure and safeguard electronically stored, personally identifiable information ("PII") and protected health information ("PHI") that Defendants shared between themselves, including,

without limitation, full names, birthdates,[1] and prescription information.[2]

2. CaptureRx is a specialty pharmacy benefits manager.[3] Its services include prescription claims processing, patient assistance program administration, and public health service 340B drug program administration. CaptureRx provides these services for pharmacies and healthcare providers across the United States, including Defendant Rite Aid.

3. Individuals entrust Defendants with an extensive amount of their PII and PHI. Defendants assert that they understand the importance of protecting such information, and that "Data privacy and security are among CaptureRx's highest priorities."

4. On or before February 11, 2021, Defendant CaptureRx learned that an unauthorized actor breached its system and accessed the electronic files containing the PII and PHI of Defendant Rite Aid's customers, including Plaintiff's and Class Members' data (the "Data Breach"). The data included, at least, Plaintiff's and Class Members' names, dates of birth and prescription information.

5. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' PII and PHI, Defendant assumed legal and equitable duties to those individuals.

6. The exposed PII and PHI of Plaintiff and Class Members can be sold on the dark web. Hackers can access and then offer for sale the unencrypted, unredacted PII and PHI to

---

[1] Personally identifiable information generally incorporates information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information. 2 C.F.R. § 200.79. At a minimum, it includes all information that on its face expressly identifies an individual.

[2] Health information including diagnoses, treatment information, medical test results, and prescription information are considered protected health information under the Health Insurance Portability and Accountability Act ("HIPAA"). *See* https://www.cdc.gov/phlp/publications/topic/hipaa.html#one.

[3] Exhibit A (*Notice of Data Event to the Washington State Attorney General*, dated May 5, 2021, also available at: https://agportal-s3bucket.s3.amazonaws.com/Data_Breach/NECNetworksDbaCaptureRx.2021-05-05.pdf.)

criminals. Plaintiff and Class Members face a lifetime risk of identity theft, which is heightened here by the loss of their birthdates and specific medical treatment information in the form of prescription information.

7. This PII and PHI was compromised due to Defendants' negligent and/or careless acts and omissions and the failure to protect the PII and PHI of Plaintiff and Class Members.

8. Plaintiff brings this action on behalf of all persons whose PII and PHI was compromised as a result of Defendants' failure to: (i) adequately protect the PII and PHI of Plaintiff and Class Members; (ii) warn Plaintiff and Class Members of their inadequate information security practices; and (iii) avoid sharing the PII and PHI of Plaintiff and Class Members without adequate safeguards. Defendants' conduct amounts to negligence and violates federal and state statutes.

9. Plaintiff and Class Members have suffered injury as a result of Defendants' conduct. These injuries include: (i) lost or diminished value of PII and PHI; (ii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their PII and PHI; (iii) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time, and significantly (iv) the continued and certainly an increased risk to their PII and PHI, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) may remain backed up in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PII and PHI.

10. Defendant disregarded the rights of Plaintiff and Class Members by intentionally, willfully, recklessly, or negligently failing to take and implement adequate and reasonable measures to ensure that Plaintiff's and Class Members' PII and PHI was safeguarded, failing to take available steps to prevent an unauthorized disclosure of data, and failing to follow applicable,

required and appropriate protocols, policies and procedures regarding the encryption of data, even for internal use. As a result, the PII and PHI of Plaintiff and Class Members was compromised through disclosure to an unknown and unauthorized third party. Plaintiff and Class Members have a continuing interest in ensuring that their information is and remains safe, and they should be entitled to injunctive and other equitable relief.

## PARTIES

11. Plaintiff Daisy Trujillo is a citizen of California residing in Merced County, California.

12. NEC Networks, LLC, d/b/a CaptureRx, is a Texas limited liability company with its principle place of business in San Antonio, Texas.

13. Rite Aid Corporation is incorporated in Delaware with its principle place of business in Camp Hill, Pennsylvania.

14. The true names and capacities of persons or entities, whether individual, corporate, associate, or otherwise, who may be responsible for some of the claims alleged herein are currently unknown to Plaintiff. Plaintiff will seek leave of court to amend this complaint to reflect the true names and capacities of such other responsible parties when their identities become known.

15. All of Plaintiff's claims stated herein are asserted against Defendants and any of their owners, predecessors, successors, subsidiaries, agents and/or assigns.

## JURISDICTION AND VENUE

16. This Court has subject matter jurisdiction over this action under 28 U.S.C. § 1332(d)(2) because this is a class action wherein the amount of controversy exceeds the sum or value of $5 million, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one member of the class is a citizen of a state different from Defendant. Plaintiff is a citizen of California and therefore diverse from Defendant CaptureRx, which is

headquartered in Texas, and Defendant Rite Aid, which is headquartered in Pennsylvania.

17. This Court has personal jurisdiction over Defendant CaptureRx because CaptureRx is a Texas LLC with its principal place of business within this District. On information and belief, some members of this limited liability company are also residents of Texas.

18. Defendant Rite Aid is subject to the personal jurisdiction of the Court because it does or transacts business in, has agents in, or is otherwise found in and has purposely availed itself of the privilege of doing business in Texas and in this District, and because the alleged misconduct was directed to Texas and this District, among others.

19. Venue is proper in this District pursuant to 28 U.S.C. § 1391(b)(2) because a substantial part of the events or omissions giving rise to the claims occurred or were intentionally directed to residents and customers in this District.

## FACTUAL ALLEGATIONS

***Background***

20. Defendant Rite Aid contracted with Defendant CaptureRx to process claims related to Rite Aid's pharmacy business. The electronic files stored and/or shared by Defendants contained non-redacted and non-encrypted PII and PHI belonging to Plaintiff and Class Members. This sensitive and confidential PII, including, but not limited to, full names and birthdates, is static and does not change, and can be used to commit myriad identity crimes. The PHI involved—pharmacy information—is also sensitive and confidential, and is protected, private medical treatment information that divulges not only the types of pharmaceuticals Plaintiff and Class Members were prescribed, but also the underlying mental or physical diagnoses.

21. Plaintiff and Class Members relied on these sophisticated Defendants to keep their PII and PHI confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information. Plaintiff and Class Members

demand security to safeguard their PII and PHI.

22. Defendants had a duty to adopt reasonable measures to protect Plaintiff's and Class Members' PII and PHI from involuntary disclosure to third parties.

***The Data Breach***

23. On or about May 5, 2021, Defendants announced that they experienced the Data Breach.[4] Defendants sent notice letters to various States' Attorneys General and to individuals impacted by the Data Breach. The Notice to Plaintiff, for example, stated:

> CaptureRx is a vendor that provides services to certain healthcare providers, including Rite Aid Corporation (together with its affiliates, 'Rite Aid'). CaptureRx is writing, on behalf of Rite Aid to notify you of a recent event at CaptureRx that may affect the privacy of some of your personal information.[5]

24. Also in the notice to impacted individuals, Defendants stated:

> **What Happened?** CaptureRx recently became aware of unusual activity involving certain of its electronic files. Following this, CaptureRx immediately began an investigation into this activity and worked quickly to assess the security of its system. On February 19, 2021, the investigation determined that certain files were accessed and acquired on February 6, 2021 without authorization. CaptureRx immediately began a thorough review of the full contents of the files to determine whether sensitive information was present at the time of the incident. On or around March 19, 2021, CaptureRx confirmed that some of your information was present in the relevant files. CaptureRx began the process of notifying Rite Aid on or around March 30, 2021 of this incident.
>
> **What Information Was Involved?** The investigation determined that, at the time of the incident, the relevant files contained your first name, last name, date of birth, and prescription information. We are providing you this notice to ensure you are aware of this incident.
> …
>
> **What You Can Do.** We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements and explanation of benefits forms, and to monitor your free credit reports for suspicious activity and to detect errors. Please also review the information contained in the attached "Steps You Can Take to Protect Personal Information.

*Id*.

[4] *See* Exhibit A.

[5] Exhibit B (Redacted *Notice of Security Incident*, dated May 5, 2021).

25. Defendant admits that an unauthorized party "accessed and acquired" electronic files that contained sensitive PII and PHI belonging to Plaintiff and Class Members. Defendants also admit that the PII and PHI included "first name, last name, date of birth, and prescription information[.]"

26. In response to the Data Breach, Defendants claim that they are "working to implement additional safeguards and training to its employees."[6] However, the details of the root cause of the Data Breach, the vulnerabilities exploited, and the remedial measures undertaken to ensure a breach does not occur again have not been shared with the states' Attorneys General or Plaintiff and Class Members, who retain a vested interest in ensuring that their information remains protected. Instead, Defendants shifted the burden of protecting their sensitive PII and PHI to Plaintiff and Class members by warning them in the Notice to now "remain vigilant against incidents of identity theft and fraud, to review your account statements and explanation of benefits forms, and to monitor your free credit reports for suspicious activity and to detect errors."[7]

27. Plaintiff's and Class Members' non-encrypted information may end up for sale on the dark web, or simply fall into the hands of companies that will use the detailed PII and PHI for targeted marketing without the approval of Plaintiff and Class Members. Because of this Data Breach, unauthorized individuals can easily access the PII and PHI of Plaintiff and Class Members.

28. Defendants did not use reasonable security procedures and practices appropriate to the nature of the sensitive, non-encrypted information it was maintaining for Plaintiff and Class Members, causing their PII and PHI to be exposed.

[6] Exhibit A.
[7] Exhibit B.

***Defendant Acquires, Collects and Stores Plaintiff's and Class Members' PII and PHI.***

29. Defendants acquired, collected, and stored Plaintiff's and Class Members' PII and PHI.

30. As a condition of its relationships with Plaintiff and Class Members, Defendants required that Plaintiff and Class Members entrust Defendants with highly sensitive, confidential PII and PHI.

31. By obtaining, collecting, and storing the PII and PHI of Plaintiff and Class Members, Defendants assumed legal and equitable duties and knew or should have known that they were responsible for protecting the PII and PHI from disclosure.

32. Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality of their PII and PHI and relied on Defendants to keep their PII and PHI confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

***Securing PII and PHI and Preventing Breaches***

33. Defendants could have prevented this Data Breach by properly securing and encrypting the PII and PHI of Plaintiff and Class Members. Alternatively, Defendants could have destroyed the data that was no longer useful, especially outdated data.

34. Defendants' negligence in safeguarding the PII and PHI of Plaintiff and Class Members is exacerbated by the repeated warnings and alerts directed to protecting and securing sensitive data.

35. Despite the prevalence of public announcements of data breach and data security compromises, Defendants failed to take appropriate steps to protect the PII and PHI of Plaintiff and Class Members from being compromised.

***Defendants Conduct Violates FTC Regulation***

36. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[8] The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."[9]

37. The ramifications of Defendants' failure to keep secure the PII and PHI of Plaintiff and Class Members are long lasting and severe. Once PII and PHI is stolen, particularly birth dates and prescription information, fraudulent use of that information and damage to victims may continue for years.

***Defendants Failed to Comply with HIPAA Standards of Conduct***

38. HIPAA requires covered entities to protect against reasonably anticipated threats to the security of PHI. Covered entities must implement safeguards to ensure the confidentiality, integrity, and availability of PHI. Safeguards must include physical, technical, and administrative components.[10]

39. Title II of HIPAA contains what are known as the Administrative Simplification provisions. 42 U.S.C. §§ 1301, *et seq*. These provisions require, among other things, that the

[8] 17 C.F.R. § 248.201 (2013).
[9] *Id*.
[10] HIPAA Journal, *What is Considered Protected Health Information Under HIPAA?*, *available at:* https://www.hipaajournal.com/what-is-considered-protected-health-information-under-hipaa/ (last visited May 27, 2021).

Department of Health and Human Services ("HHS") create rules to streamline the standards for handling the type of PII and related data that Defendants left unguarded. The HHS has subsequently promulgated five rules under authority of the Administrative Simplification provisions of HIPAA.

40. The HIPAA Breach Notification Rule, 45 C.F.R. §§ 164.400-414, required Defendants to provide notice of the breach to each affected individual "without unreasonable delay and ***in no case later than 60 days following discovery of the breach***."[11]

41. Based on information and belief, Defendants' Data Breach resulted from a combination of insufficiencies that demonstrate Defendants failed to comply with safeguards mandated by HIPAA regulations. Defendants' security failures include, but are not limited to, the following:

a. Failing to ensure the confidentiality and integrity of electronic PHI that Defendants create, receive, maintain, and transmit in violation of 45 C.F.R. §164.306(a)(1);

b. Failing to implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights in violation of 45 C.F.R. §164.312(a)(1);

c. Failing to implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 C.F.R. §164.308(a)(1);

d. Failing to identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the

[11] Breach Notification Rule, U.S. Dep't of Health & Human Services, *available at:* https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html (emphasis added) (last visited May 27, 2021).

covered entity in violation of 45 C.F.R. §164.308(a)(6)(ii);

e. Failing to protect against any reasonably-anticipated threats or hazards to the security or integrity of electronic PHI in violation of 45 C.F.R. §164.306(a)(2);

f. Failing to protect against any reasonably anticipated uses or disclosures of electronically PHI that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 C.F.R. §164.306(a)(3);

g. Failing to ensure compliance with HIPAA security standard rules by their workforce in violation of 45 C.F.R. §164.306(a)(4);

h. Impermissibly and improperly using and disclosing PHI that is and remains accessible to unauthorized persons in violation of 45 C.F.R. §164.502, *et seq*.;

i. Failing to effectively train all members of their workforce (including independent contractors) on the policies and procedures with respect to PHI as necessary and appropriate for the members of their workforce to carry out their functions and to maintain security of PHI in violation of 45 C.F.R. §164.530(b) and 45 C.F.R. §164.308(a)(5); and

j. Failing to design, implement, and enforce policies and procedures establishing physical and administrative safeguards to reasonably safeguard PHI, in compliance with 45 C.F.R. §164.530(c).

***Value of Personal Identifiable Information***

42. It is well known that PII and PHI are invaluable commodities[12] and the frequent target of hackers. In 2019, a record 1,473 data breaches occurred, resulting in approximately

[12] *See, e.g.*, John T. Soma, et al, *Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets*, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

164,683,455 sensitive records being exposed, a 17% increase from 2018.[13] Of the 1,473 recorded data breaches, 525 of them, or 35.64%, were in the medical or healthcare industry.[14] The 525 reported breaches reported in 2019 exposed nearly 40 million sensitive records (39,378,157), compared to only 369 breaches that exposed just over 10 million sensitive records (10,632,600) in 2018.[15]

43. Consumers place a high value not only on their PII, but also on the privacy of that data. This is because identity theft causes significant negative financial impact on victims as well as severe distress and other strong emotions and physical reactions.

44. Defendants were well aware that the PII and PHI they collect is highly sensitive and of significant value to those who would use it for wrongful purposes. PII and PHI is a valuable commodity to identity thieves. As the FTC recognizes, identity thieves can use this information to commit an array of crimes including identify theft, and medical and financial fraud.[16] Indeed, a robust "cyber black market" exists in which criminals openly post stolen PII and PHI on multiple underground Internet websites, commonly referred to as the dark web.

45. There is a market for Plaintiff's and Class Members PII and PHI, and the stolen PII and PHI has inherent value. Sensitive healthcare data can sell for as much as $363 per record according to the Infosec Institute.[17]

46. PHI is particularly valuable because criminals can use it to target victims with

---

[13] https://www.idtheftcenter.org/wp-content/uploads/2020/01/01.28.2020_ITRC_2019-End-of-Year-Data-Breach-Report_FINAL_Highres-Appendix.pdf (last visited June 2, 2021)
[14] *Id*.
[15] *Id* at p15.
[16] Federal Trade Commission, *Warning Signs of Identity Theft, available at:* https://www.consumer.ftc.gov/articles/0271-warning-signs-identity-theft (last visited May 27, 2021).
[17] *See* Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, InfoSec (July 27, 2015), *available at:* https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/ (last visited May 29, 2021)

frauds and scams that take advantage of the victim's medical conditions or victim settlements. It can be used to create fake insurance claims, allowing for the purchase and resale of medical equipment, or gain access to prescriptions for illegal use or resale.

47. Drug manufacturers, medical device manufacturers, pharmacies, hospitals and other healthcare service providers often purchase PII and PHI on the black market for the purpose of target marketing their products and services to the physical maladies of the data breach victims themselves. Insurance companies purchase and use wrongfully disclosed PHI to adjust their insureds' medical insurance premiums.

48. Medical identify theft can result in inaccuracies in medical records and costly false claims. It can also have life-threatening consequences. If a victim's health information is mixed with other records, it can lead to misdiagnosis or mistreatment. "Medical identity theft is a growing and dangerous crime that leaves its victims with little to no recourse for recovery," reported Pam Dixon, executive director of World Privacy Forum. "Victims often experience financial repercussions and worse yet, they frequently discover erroneous information has been added to their personal medical files due to the thief's activities."[18]

49. Similarly, the FBI Cyber Division, in an April 8, 2014 Private Industry Notification, advised:

> Cyber criminals are selling [medical] information on the black market at a rate of $50 for each partial EHR, compared to $1 for a stolen social security number or credit card number. EHR can then be used to file fraudulent insurance claims, obtain prescription medication, and advance identity theft. EHR theft is also more difficult to detect, taking almost twice as long as normal identity theft.[19]

---

[18] Michael Ollove, "The Rise of Medical Identity Theft in Healthcare," Kaiser Health News, Feb. 7, 2014, *available at:* https://khn.org/news/rise-of-indentity-theft/ (last visited May 27, 2021).

[19] FBI Cyber Division, Private Industry Notification, "(U) Health Care Systems and Medical Devices at Risk for Increased Cyber Intrusions for Financial Gain," Apr. 8, 2014, *available at:* http://www.illuminweb.com/wp-content/uploads/ill-mo-uploads/103/2418/health-systems-cyber-intrusions.pdf (last visited June 2, 2021).

50. The ramifications of Defendants' failure to keep its customers' PII and PHI secure are long lasting and severe. Once PII and PHI is stolen, fraudulent use of that information and damage to victims may continue for years. Fraudulent activity might not show up for six to 12 months or even longer.

51. Further, criminals often trade stolen PII and PHI on the "cyber black market" for years following a breach. Cybercriminals can post stolen PII and PHI on the internet, thereby making such information publicly available.

52. Defendants knew, or should have known, the importance of safeguarding the PII and PHI entrusted to it and of the foreseeable consequences if its data security systems were breached. This includes the significant costs that would be imposed on Defendants' clients as a result of a breach. Defendants failed, however, to take adequate cybersecurity measures to prevent the Data Breach.

***Plaintiff Daisy Trujillo's Experience***

53. From approximately 2005 to the present, Plaintiff Trujillo has been a customer of Rite Aid Corp.

54. On or around May 5, 2021, Plaintiff Trujillo received the Notice of Security Incident from CaptureRx informing her of the Data breach.

55. The Notice of Security Incident letter notified Plaintiff Trujillo that her first name, last name, date of birth, and prescription information may have been exposed.

56. After the Data Breach, Plaintiff Trujillo's cell phone was inundated with spam telephone calls. Her email account was also flooded with spam emails that she did not want to receive.

57. As a result of the Data Breach, Plaintiff Trujillo spent time dealing with the

consequences of the Data Breach, which includes time spent on the telephone and sorting through her unsolicited emails, verifying the legitimacy of the Data Breach, exploring credit monitoring and identity theft insurance options, and self-monitoring her accounts. This time has been lost forever and cannot be recaptured.

58. Additionally, Plaintiff Trujillo is very careful about sharing her PII and PHI. She has never knowingly transmitted unencrypted PII or PHI over the internet or any other unsecured source.

59. Plaintiff Trujillo stores any documents containing her PII and PHI in a safe and secure location. Moreover, she diligently chooses unique usernames and passwords for her few online accounts.

60. Plaintiff Trujillo suffered actual injury in the form of damages to and diminution in the value of her PII and PHI—a form of intangible property that she entrusted to Defendant for the purpose of obtaining her prescription medication, which was compromised in and as a result of the Data Breach.

61. Plaintiff Trujillo suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of her privacy, as well as anxiety over possibly losing access to her necessary prescription medications.

62. Plaintiff Trujillo has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from her PII and PHI, especially her medical information, in combination with her name, being placed in the hands of unauthorized third-parties and possibly criminals.

63. Plaintiff Trujillo has a continuing interest in ensuring that her PII and PHI, which, upon information and belief, remains backed up in Defendant's possession, is protected and

safeguarded from future breaches.

## CLASS ALLEGATIONS

64. Plaintiff brings this nationwide class action on behalf of herself and on behalf of all others similarly situated pursuant to Code of Civil Procedure § 382, Civil Code § 1781, and other applicable law.

65. The Nationwide Class that Plaintiff seeks to represent is defined as follows:

> All individuals residing in the United States whose PII and PHI (a) Defendants stored and/or shared in Defendant CaptureRx's electronic files and (b) was exposed to an unauthorized party as a result of the data breach announced on May 5, 2021 (the "Nationwide Class").

66. In addition to claims asserted on behalf of the Nationwide Class, Plaintiff asserts claims on behalf of a separate California subclass, defined as follows:

> All individuals residing in California whose PII and PHI (a) Defendants stored and/or shared in Defendant CaptureRx's electronic files and (b) was exposed to an unauthorized party as a result of the data breach announced on May 5, 2021 (the "California Class").

67. Excluded from the Classes are the following individuals and/or entities: Defendants and Defendants' parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendant has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; any and all federal, state or local governments, including but not limited to their departments, agencies, divisions, bureaus, boards, sections, groups, counsels and/or subdivisions; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

68. Plaintiff reserves the right to modify or amend the definition of the proposed classes before the Court determines whether certification is appropriate.

69. This action is brought and may be maintained as a class action because there is a well-defined community of interest among many persons who comprise a readily ascertainable class. A well-defined community of interest exists to warrant class wide relief because Plaintiff and all members of the Nationwide Class were subjected to the same wrongful practices by Defendant, entitling them to the same relief.

70. The Nationwide Class is so numerous that individual joinder of its members is impracticable. While the exact number of Class Members is unknown to Plaintiff at this time, Plaintiff is informed and believes that there are at least hundreds of thousands of Class Members.[20]

71. Common questions of law and fact exist as to members of the Nationwide Class and predominate over any questions which affect only individual members of the Class. These common questions include, but are not limited to:

a. Whether and to what extent Defendants had a duty to protect the PII and PHI of Plaintiff and Class Members;

b. Whether Defendants had a duty not to disclose the PII and PHI of Plaintiff and Class Members to unauthorized third parties;

c. Whether Defendants had a duty not to use the PII and PHI of Plaintiff and Class Members for non-business purposes;

d. Whether Defendants failed to adequately safeguard the PII and PHI of Plaintiff and Class Members;

e. Whether and when Defendants actually learned of the Data Breach;

f. Whether Defendants adequately, promptly, and accurately informed Plaintiff and

[20] Defendant CaptureRx reported to the Maine Attorney General that 1,919,938 people were impacted by the Data Breach. *See* Exhibit C (Data Breach Notifications, also available at: https://apps.web.maine.gov/online/aeviewer/ME/40/e8aa9ab4-e354-44db-b730-e002aca8955d.shtml (last visited May 27, 2021)).

Class Members that their PII and PHI had been compromised;

g. Whether Defendants violated the law by failing to promptly notify Plaintiff and Class Members that their PII and PHI had been compromised;

h. Whether Defendants failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

i. Whether Defendants adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

j. Whether Defendants engaged in unfair, unlawful, or deceptive practices by failing to safeguard the PII and PHI of Plaintiff and Class Members;

k. Whether Plaintiff and Class Members are entitled to actual, damages, and/or statutory damages as a result of Defendants' wrongful conduct;

l. Whether Plaintiff and Class Members are entitled to restitution as a result of Defendants' wrongful conduct; and

m. Whether Plaintiff and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach.

72. Plaintiff is a member of the Classes she seeks to represent and her claims and injuries are typical of the claims and injuries of the other Class Members.

73. Plaintiff will adequately and fairly protect the interests of other Class Members. Plaintiff has no interests adverse to the interests of absent Class Members. Plaintiff is represented by legal counsel with substantial experience in class action litigation. The interests of Class Members will be fairly and adequately protected by Plaintiff and their counsel.

74. Defendants have acted or refused to act on grounds that apply generally to the Class

Members, so that final injunctive relief or corresponding declaratory relief is appropriate respecting the Class as a whole.

75. A class action is superior to other available means for fair and efficient adjudication of the claims of the Class and would be beneficial for the parties and the court. Class action treatment will allow a large number of similarly situated persons to prosecute their common claims in a single forum, simultaneously, efficiently, and without the unnecessary duplication of effort and expense that numerous individual actions would require. The amounts owed to the many individual Class Members are likely to be relatively small, and the burden and expense of individual litigation would make it difficult or impossible for individual members of the class to seek and obtain relief. A class action will serve an important public interest by permitting such individuals to effectively pursue recovery of the sums owed to them. Further, class litigation prevents the potential for inconsistent or contradictory judgments raised by individual litigation. Plaintiff are unaware of any difficulties that are likely to be encountered in the management of this action that would preclude its maintenance as a class action.

**COUNT I**
**Negligence**
**(On Behalf of Plaintiff and the Nationwide Class)**

76. Plaintiff and the Nationwide Class re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 75.

77. Plaintiff and the Nationwide Class provided and entrusted Defendants with certain PII and PHI, including but not limited to their full names, birthdates, and medical information, including pharmaceutical prescriptions.

78. Plaintiff and the Nationwide Class entrusted their PII and PHI to Defendants on the premise and with the understanding that Defendants would safeguard their information, use their

PII and PHI for business purposes only, and/or not disclose their PII and PHI to unauthorized third parties.

79. Defendants have full knowledge of the sensitivity of the PII and PHI and the types of harm that Plaintiff and the Nationwide Class could and would suffer if the PII and PHI were wrongfully disclosed.

80. Defendants knew or reasonably should have known that the failure to exercise due care in the collecting, storing, and using of the PII and PHI of Plaintiff and the Nationwide Class involved an unreasonable risk of harm to Plaintiff and the Nationwide Class, even if the harm occurred through the criminal acts of a third party.

81. Defendants had a duty to exercise reasonable care in safeguarding, securing, and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties. This duty includes, among other things, designing, maintaining, and testing Defendants' security protocols to ensure that the PII and PHI of Plaintiff and the Nationwide Class in Defendants' possession was adequately secured and protected.

82. Defendants also had a duty to exercise appropriate clearinghouse practices to remove PII and PHI it was no longer required to retain pursuant to regulations.

83. Defendants also had a duty to have procedures in place to detect and prevent the improper access and misuse of the PII and PHI of Plaintiff and the Nationwide Class.

84. Defendants' duty to use reasonable security measures arose as a result of the special relationship that existed between Defendants and Plaintiff and the Nationwide Class, which is recognized by laws and regulations including but not limited to HIPAA, as well as the common law. That special relationship arose because Plaintiff and the Nationwide Class entrusted Defendants with their confidential PII and PHI, a necessary part of their relationships with

Defendants.

85. Defendants' duty to use reasonable security measures under HIPAA required Defendants to "reasonably safeguard" confidential data from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. § 164.530(c).

86. Some or all of the medical information at issue in this case constitutes "protected health information" within the meaning of HIPAA.

87. In addition, Defendants had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

88. Defendants were subject to an "independent duty," untethered to any contract between Defendants and Plaintiff or the Nationwide Class.

89. A breach of security, unauthorized access, and resulting injury to Plaintiff and the Nationwide Class was reasonably foreseeable, particularly in light of Defendants' inadequate security practices, including sharing and/or storing the PII and PHI of Plaintiff and the Nationwide Class on its computer systems.

90. Plaintiff and the Nationwide Class were the foreseeable and probable victims of any inadequate security practices and procedures. Defendants knew or should have known of the inherent risks in collecting and storing the PII and PHI of Plaintiff and the Nationwide Class, the critical importance of providing adequate security of that PII and PHI, and the necessity for encrypting PII and PHI stored on Defendants' systems.

91. Defendants' own conduct created a foreseeable risk of harm to Plaintiff and the

Nationwide Class. Defendants' misconduct included, but was not limited to, their failure to take the steps and opportunities to prevent the Data Breach as set forth herein. Defendants' misconduct also included their decisions not to comply with industry standards for the safekeeping of the PII and PHI of Plaintiff and the Nationwide Class, including basic encryption techniques freely available to Defendants.

92. Plaintiff and the Nationwide Class had no ability to protect their PII and PHI that was in, and possibly remains in, Defendants' possession.

93. Defendants were in a position to protect against the harm suffered by Plaintiff and the Nationwide Class as a result of the Data Breach.

94. Defendants had and continue to have a duty to adequately disclose that the PII and PHI of Plaintiff and the Nationwide Class within Defendants' possession might have been compromised, how it was compromised, and precisely the types of data that were compromised and when. Such notice was necessary to allow Plaintiff and the Nationwide Class to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their PII by third parties.

95. Defendants had a duty to employ proper procedures to prevent the unauthorized dissemination of the PII and PHI of Plaintiff and the Nationwide Class.

96. Defendants admitted that the PII and PHI of Plaintiff and the Nationwide Class was wrongfully "accessed and acquired" by unauthorized actors as a result of the Data Breach.

97. Defendants, through their actions and/or omissions, unlawfully breached their duties to Plaintiff and the Nationwide Class by failing to implement industry protocols and exercise reasonable care in protecting and safeguarding the PII and PHI of Plaintiff and the Nationwide Class during the time the PII and PHI were within Defendants' possession or control.

98. Defendants improperly and inadequately safeguarded the PII and PHI of Plaintiff

and the Nationwide Class in deviation of standard industry rules, regulations, and practices at the time of the Data Breach, including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2 of the NIST Cybersecurity Framework Version 1.1.

99. Defendants failed to heed industry warnings and alerts to provide adequate safeguards to protect the PII and PHI of Plaintiff and the Nationwide Class in the face of increased risk of theft.

100. Defendants, through their actions and/or omissions, unlawfully breached their duty to Plaintiff and the Nationwide Class by failing to have appropriate procedures in place to detect and prevent dissemination of their PII and PHI.

101. Defendants breached their duty to exercise appropriate clearinghouse practices by failing to remove PII and PHI that was no longer required to retain pursuant to regulations.

102. Defendants, through its actions and/or omissions, unlawfully breached their duty to adequately and timely disclose to Plaintiff and the Nationwide Class the existence and scope of the Data Breach.

103. But for Defendants' wrongful and negligent breach of duties owed to Plaintiff and the Nationwide Class, the PII and PHI of Plaintiff and the Nationwide Class would not have been compromised.

104. There is a close causal connection between Defendants' failure to implement security measures to protect the PII and PHI of Plaintiff and the Nationwide Class and the harm, or risk of imminent harm, suffered by Plaintiff and the Nationwide Class. The PII and PHI of Plaintiff and the Nationwide Class was lost and accessed as the proximate result of Defendants' failure to exercise reasonable care in safeguarding such PII and PHI by adopting, implementing,

and maintaining appropriate security measures.

105. Additionally, Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect PII. The FTC publications and orders described above also form part of the basis of Defendant's duty in this regard.

106. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with applicable industry standards, as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of PII it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiff and the Nationwide Class.

107. Defendant's violation of Section 5 of the FTC Act constitutes negligence *per se*.

108. Plaintiff and the Nationwide Class are within the class of persons that the FTC Act was intended to protect.

109. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and the Nationwide Class.

110. Defendants' misconduct also included their decision not to comply with HIPAA for the reporting, safekeeping and encrypted authorized disclosure of the PHI of Plaintiff and Class Members.

111. HIPAA privacy laws were enacted with the objective of protecting the confidentiality of patients' healthcare information and set forth the conditions under which such

information can be used, and to whom it can be disclosed. HIPAA privacy laws not only apply to healthcare providers and the organizations they work for, but to any entity that may have access to healthcare information about a patient that—if it were to fall into the wrong hands—could present a risk of harm to the patient's finances or reputation.

112. Plaintiff and Class Members are within the class of persons that HIPAA privacy laws were intended to protect.

113. The harm that occurred as a result of the Data Breach is the type of harm HIPAA privacy laws were intended to guard against.

114. As a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiff and the Nationwide Class have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity of how their PII and PHI is used; (iii) the compromise, publication, and/or theft of their PII and PHI; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PI and PHI I; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their PII and PHI, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII of Plaintiff and the Nationwide Class; and (viii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and the Nationwide Class.

115. As a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiff and the Nationwide Class have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

116. Additionally, as a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiff and the Nationwide Class have suffered and will suffer the continued risks of exposure of their PII and PHI, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII in its continued possession.

**COUNT II**
**Breach of Implied Contract**
**(On Behalf of Plaintiff and the Nationwide Class)**

117. Plaintiff and the Nationwide Class re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 75.

118. Through their course of conduct, Defendants, Plaintiff, and Class Members entered into implied contracts for the Defendant to implement data security adequate to safeguard and protect the privacy of Plaintiff's and Class Members' PII and PHI.

119. Defendants required Plaintiff and the Nationwide Class to provide and entrust their PII and PHI, including full names, birthdates and prescription information and/or other information, as a condition of getting their prescriptions filled by Defendant Rite Aid and processed by Defendant CaptureRx.

120. Defendant Rite Aid solicited and invited Plaintiff and the Class Members to provide their PII and PHI as part of Defendant Rite Aid's regular business practices. Plaintiff and Class

Members accepted Defendant Rite Aid's offers and provided their PII and PHI to Defendant Rite Aid.

121. As a condition of being customers of Defendants, Plaintiff and the Nationwide Class provided and entrusted their PII and PHI to Defendants. In so doing, Plaintiff and the Class entered into implied contracts with Defendants by which Defendants agreed to safeguard and protect such non-public information, to keep such information secure and confidential, and to timely and accurately notify Plaintiff and the Nationwide Class if their data had been breached and compromised or stolen.

122. A meeting of the minds occurred when Plaintiff and the Class Members agreed to, and did, provide their PII and PHI to Defendants, in exchange for, amongst other things, the protection of their Private Information.

123. Plaintiff and the Nationwide Class fully performed their obligations under the implied contracts with Defendants.

124. Defendants breached the implied contracts it made with Plaintiff and the Nationwide Class by failing to safeguard and protect their PII and PHI by failing to provide timely and accurate notice to them that their PII and PHI was compromised as a result of the Data Breach.

125. As a direct and proximate result of Defendants' above-described breach of implied contract, Plaintiff and the Nationwide Class have suffered (and will continue to suffer) ongoing, imminent, and impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; loss of the confidentiality of the stolen confidential data; the illegal sale of the compromised data on the dark web; expenses and/or time spent on credit monitoring and identity theft insurance; time spent scrutinizing bank statements, credit card statements, and credit

reports; expenses and/or time spent initiating fraud alerts, decreased credit scores and ratings; lost work time; and other economic and non-economic harm.

**COUNT III**
**Invasion of Privacy**
**(On Behalf of Plaintiff and the Nationwide Class)**

126. Plaintiff and the Nationwide Class re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 75.

127. Plaintiff and the Nationwide Class had a legitimate expectation of privacy to their PII and PHI and were entitled to the protection of this information against disclosure to unauthorized third parties.

128. Defendants owed a duty to Plaintiff and the Nationwide Class to keep their PII and PHI contained as a part thereof, confidential.

129. Defendants failed to protect and released to unknown and unauthorized third parties the non-redacted and non-encrypted PII and PHI of Plaintiff and the Nationwide Class.

130. Defendants allowed unauthorized and unknown third parties access to and examination of the PII and PHI of Plaintiff and the Nationwide Class, by way of Defendants' failure to protect the PII and PHI.

131. The unauthorized release to, custody of, and examination by unauthorized third parties of the PII and PHI of Plaintiff and the Nationwide Class is highly offensive to a reasonable person.

132. The intrusion was into a place or thing, which was private and is entitled to be private. Plaintiff and the Nationwide Class disclosed their PII and PHI to Defendants as part of Plaintiff's and the Nationwide Class's relationships with Defendants, but privately with an intention that the PII and PHI would be kept confidential and would be protected from

unauthorized disclosure. Plaintiff and the Nationwide Class were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization.

133. The Data Breach at the hands of Defendants constitutes an intentional interference with Plaintiff's and the Nationwide Class's interest in solitude or seclusion, either as to their persons or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

134. Defendants acted with a knowing state of mind when it permitted the Data Breach to occur because it was with actual knowledge that its information security practices were inadequate and insufficient.

135. Because Defendants acted with this knowing state of mind, it had notice and knew the inadequate and insufficient information security practices would cause injury and harm to Plaintiff and the Nationwide Class.

136. As a proximate result of the above acts and omissions of Defendants, the PII and PHI of Plaintiff and the Nationwide Class was disclosed to third parties without authorization, causing Plaintiff and the Nationwide Class to suffer damages.

137. Unless and until enjoined, and restrained by order of this Court, Defendants' wrongful conduct will continue to cause great and irreparable injury to Plaintiff and the Nationwide Class in that the PII and PHI maintained by Defendants can be viewed, distributed, and used by unauthorized persons for years to come. Plaintiff and the Nationwide Class have no adequate remedy at law for the injuries in that a judgment for monetary damages will not end the invasion of privacy for Plaintiff and the Nationwide Class.

**COUNT IV**
**Breach of Confidence**
**(On Behalf of Plaintiff and the Nationwide Class Against Defendant Rite Aid)**

138. Plaintiff and the Nationwide Class re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 75.

139. At all times during Plaintiff's and the Nationwide Class's interactions with Defendant Rite Aid, Defendant was fully aware of the confidential and sensitive nature of Plaintiff's and the Nationwide Class's PII that Plaintiff and the Nationwide Class provided to Defendant.

140. As alleged herein and above, Defendant's relationship with Plaintiff and the Nationwide Class was governed by terms and expectations that Plaintiff's and the Nationwide Class's PII would be collected, stored, and protected in confidence, and would not be disclosed to unauthorized third parties.

141. Plaintiff and the Nationwide Class provided their PII to Defendant Rite Aid with the explicit and implicit understandings that Defendant would protect and not permit the PII to be disseminated to any unauthorized third parties.

142. Plaintiff and the Nationwide Class also provided their PII to Defendant Rite Aid with the explicit and implicit understandings that Defendant would take precautions to protect that PII from unauthorized disclosure.

143. Defendant Rite Aid voluntarily received in confidence the PII of Plaintiff and the Nationwide Class with the understanding that PII would not be disclosed or disseminated to the public or any unauthorized third parties.

144. Due to Defendant Rite Aid's failure to prevent and avoid the Data Breach from occurring, the PII of Plaintiff and the Nationwide Class was disclosed and misappropriated to

unauthorized third parties beyond Plaintiff's and the Nationwide Class's confidence, and without their express permission.

145. As a direct and proximate cause of Defendant Rite Aid's actions and/or omissions, Plaintiff and the Nationwide Class have suffered damages.

146. But for Defendant Rite Aid's disclosure of Plaintiff's and the Nationwide Class's PII in violation of the parties' understanding of confidence, their PII would not have been compromised, stolen, viewed, accessed, and used by unauthorized third parties. The Data Breach was the direct and legal cause of the theft of Plaintiff's and the Nationwide Class's PII as well as the resulting damages.

147. The injury and harm Plaintiff and the Nationwide Class suffered was the reasonably foreseeable result of Defendant Rite Aid's unauthorized disclosure of Plaintiff's and the Nationwide Class's PII. Defendant knew or should have known its methods of accepting and securing Plaintiff's and the Nationwide Class's PII was inadequate as it relates to, at the very least, securing servers and other equipment containing Plaintiff's and the Nationwide Class's PII.

148. As a direct and proximate result of Defendant Rite Aid's breach of its confidence with Plaintiff and the Nationwide Class, Plaintiff and the Nationwide Class have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity how their PII and PHI is used; (iii) the compromise and/or theft of their PII and PHI; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII and PHI; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with

placing freezes on credit reports; (vii) the continued risk to their PII and PHI, which remain in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fails to undertake appropriate and adequate measures to protect the PII of Plaintiff and the Nationwide Class; and (viii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII and PHI compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and the Nationwide Class.

149. As a direct and proximate result of Defendant Rite Aid's breaches of confidence, Plaintiff and the Nationwide Class have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

**COUNT V**
**Violation of the California Unfair Competition Law,**
**Cal. Bus. & Prof. Code § 17200, *et seq*. – Unlawful Business Practices**
**(On Behalf of Plaintiff and the California Class)**

150. Plaintiff and the California Class re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 75.

151. Defendants have violated Cal. Bus. and Prof. Code § 17200, *et seq*., by engaging in unlawful, unfair or fraudulent business acts and practices and unfair, deceptive, untrue or misleading advertising that constitute acts of "unfair competition" as defined in Cal. Bus. Prof. Code § 17200 with respect to the services provided to the California Class.

152. Defendants engaged in unlawful acts and practices with respect to the services by establishing the sub-standard security practices and procedures described herein; by soliciting and collecting the PII and PHI of Plaintiff and the California Class with knowledge that the information would not be adequately protected; and by storing the PII and PHI of Plaintiff and the California Class in an unsecure environment in violation of California's data breach statute, Cal. Civ. Code

§ 1798.81.5, which requires Defendants to take reasonable methods of safeguarding the PII and PHI of Plaintiff and the California Class.

153. As a direct and proximate result of Defendants' unlawful practices and acts, Plaintiff and the California Class were injured and lost money or property, including but not limited to the price received by Defendants for the services, the loss of Plaintiff and the California Class's legally protected interest in the confidentiality and privacy of their PII and PHI, nominal damages, and additional losses as described above.

154. Defendants knew or should have known that Defendants' data security practices were inadequate to safeguard the PII and PHI of Plaintiff and the California Class and that the risk of a data breach or theft was highly likely, especially given Defendants' inability to adhere to basic encryption standards and data disposal methodologies. Defendants' actions in engaging in the above-named unlawful practices and acts were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of members of the California Class.

155. Plaintiff and the California Class seek relief under Cal. Bus. & Prof. Code § 17200, *et seq.*, including, but not limited to, restitution to Plaintiff and the California Class of money or property that Defendant may have acquired by means of Defendants' unlawful, and unfair business practices, restitutionary disgorgement of all profits accruing to Defendant because of Defendants' unlawful and unfair business practices, declaratory relief, attorneys' fees and costs (pursuant to Cal. Code Civ. Proc. § 1021.5), and injunctive or other equitable relief.

## COUNT VI
**Violation of California's Unfair Competition Law,**
**Cal. Bus. & Prof. Code § 17200, *et seq.* – Unfair Business Practices**
**(On Behalf of Plaintiff and the California Class)**

156. Plaintiff and the California Class re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 75.

157. Defendants engaged in unfair acts and practices with respect to the services by establishing the sub-standard security practices and procedures described herein by soliciting and collecting the PII and PHI of Plaintiff and the California Class with knowledge that the information would not be adequately protected and by storing the PII and PHI Plaintiff and the California Class in an unsecure electronic environment. These unfair acts and practices were immoral, unethical, oppressive, unscrupulous, unconscionable, and/or substantially injurious to Plaintiff and the California Class. They were likely to deceive the public into believing their PII and PHI was securely stored, when it was not. The harm these practices caused to Plaintiff and the California Class outweighed their utility, if any.

158. Defendants engaged in unfair acts and practices with respect to the provision of services by failing to take proper action following the Data Breach to enact adequate privacy and security measures and protect the PII and PHI of Plaintiff and the California Class from further unauthorized disclosure, release, data breaches, and theft. These unfair acts and practices were immoral, unethical, oppressive, unscrupulous, unconscionable, and/or substantially injurious to Plaintiff and the California Class. They were likely to deceive the public into believing their PII and PHI were securely stored, when they were not. The harm these practices caused to Plaintiff and the California Class outweighed their utility, if any.

159. As a direct and proximate result of Defendants' acts of unfair practices, Plaintiff and the California Class were injured and lost money or property, including but not limited to the price received by Defendants for the services, the loss of Plaintiff and the California Class's legally protected interest in the confidentiality and privacy of their PII and PHI, nominal damages, and additional losses as described above.

160. Defendants knew or should have known that Defendants' data security practices were inadequate to safeguard the PII and PHI of Plaintiff and the California Class and that the risk of a data breach or theft was highly likely, including Defendants' failure to properly encrypt files containing sensitive PII and PHI. Defendants' actions in engaging in the above-named unlawful practices and acts were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of Plaintiff and the California Class.

161. Plaintiff and the California Class seek relief under Cal. Bus. & Prof. Code § 17200, *et seq*., including, but not limited to, restitution to Plaintiff and the California Class of money or property that the Defendants may have acquired by means of Defendants' unfair business practices, restitutionary disgorgement of all profits accruing to Defendants because of Defendants' unfair business practices, declaratory relief, attorneys' fees and costs (pursuant to Cal. Code Civ. Proc. § 1021.5), and injunctive or other equitable relief.

**COUNT VII**
**Violation of the Confidentiality of Medical Information Act ("CMIA"),**
**Cal. Civ. Code §§ 56, *et seq*.**
**(On Behalf of Plaintiff and the California Class)**

162. Plaintiff and the California Class re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 75.

163. At all relevant times, Defendants were healthcare provider for the purposes of this cause of action because they had the "purpose of maintaining medical information to make the information available to an individual or to a provider of health care at the request of the individual or a provider of health care, for purposes of allowing the individual to manage his or her information, or for the diagnosis or treatment of the individual."

164. Defendants are provider of healthcare for the purposes of this cause of action within the meaning of Civil Code § 56.06(a) and maintains medical information as defined by Civil Code § 56.05.

165. Plaintiff and California Class Members are patients of Defendants for the purposes of this cause of action, as defined in Civil Code § 56.05(k).

166. Plaintiff and California Class Members provided their PII and PHI to Defendant Rite Aid, who in turn gave it to its processor Defendant CaptureRx.

167. At all relevant times, Defendants collected, stored, managed, and transmitted Plaintiff's and California Class Members' personal medical information.

168. Section 56.10(a) of the California Civil Code provides that "[a] provider of health care, health care service plan, or contractor shall not disclose medical information regarding a patient of the provider of health care or an enrollee or subscriber of a health care service plan without first obtaining an authorization."

169. As a result of the Data Breach, Defendants misused, disclosed, and/or allowed third parties to access and view Plaintiff's and Class Members' personal medical information without their written authorization compliant with the provisions of Civil Code §§ 56, *et seq*.

170. As a further result of the Data Breach, the confidential nature of the Plaintiff's and California Class Members' medical information was breached as a result of Defendant's negligence. Specifically, Defendants knowingly allowed and affirmatively acted in a manner that actually allowed unauthorized parties to access, view, and use Plaintiff's and California Class Members' PHI.

171. Defendants' misuse and/or disclosure of medical information regarding Plaintiff and California Class Members constitutes a violation of Civil Code §§ 56.10, 56.11, 56.13, and 56.26.

172. As a direct and proximate result of Defendants' wrongful actions, inaction, omissions, and want of ordinary care, Plaintiff's and California Class Members' personal medical information was disclosed without written authorization.

173. By disclosing Plaintiff's and California Class Members' PII and PHI without their written authorization, Defendants violated California Civil Code § 56, *et seq*., and their legal duties to protect the confidentiality of such information.

174. Defendants also violated Sections 56.06 and 56.101 of the California CMIA, which prohibit the negligent creation, maintenance, preservation, storage, abandonment, destruction or disposal of confidential personal medical information.

175. As a direct and proximate result of Defendants' wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused the Data Breach, Plaintiff's and California Class Members' personal medical information was viewed by, released to, and disclosed to third parties without Plaintiff's and California Class Members' written authorization.

176. As a direct and proximate result of Defendants' above-described wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused the Data Breach and its violations of the CMIA, Plaintiff and California Class Members are entitled to (i) actual damages, (ii) nominal damages of $1,000 per Plaintiff and California Class Member, (iii) punitive damages of up to $3,000 per Plaintiff and California Class Member, and (iv) attorneys' fees, litigation expenses and court costs under California Civil Code § 56.35.

**COUNT VIII**
**Violation of California's Information Practices Act of 1977,**
**Cal. Civ. Code § 1798, *et seq*.**
**(On Behalf of Plaintiff and the California Class)**

177. Plaintiff and the California Class re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 75.

178. Defendants were legally obligated to "establish appropriate and reasonable administrative, technical, and physical safeguards to ensure compliance with the [Information Practices Act of 1977], to ensure the security and confidentiality of records, and to protect against anticipated threats or hazards to their security or integrity which could result in any injury." Cal. Civ. Code § 1798.21.

179. Defendants failed to establish appropriate and reasonable administrative, technical, and physical safeguards to ensure compliance with the Information Practices Act of 1977 with regard to the PII and PHI of Plaintiff and the California Class.

180. Defendants failed to ensure the security and confidentiality of records containing the PII and PHI of Plaintiff and the California Class.

181. Defendants failed to protect against anticipated threats and hazards to the security and integrity of records containing the PII and PHI of Plaintiff and the California Class.

182. As a result of these failures, Plaintiff and the California Class have suffered (and will continue to suffer) economic damages and other injury and actual harm in the form of, *inter alia*, (i) an imminent, immediate and continuing increased risk of identity theft, identify fraud, and medical fraud - risks justifying expenditures for protective and remedial services for which they are entitled to compensation, (ii) invasion of privacy, (iii) breach of the confidentiality of their PII/PHI, (iv) deprivation of the value of their PII/PHI, for which there is a well-established national

and international market, and/or (v) the financial and temporal cost of monitoring her credit, monitoring her financial accounts, and mitigating their damages.

183. Plaintiff and the California Class are also entitled to injunctive relief under California Civil Code § 1798.47.

## PRAYER FOR RELIEF

**WHEREFORE**, Plaintiff, on behalf of herself and Class Members, request judgment against Defendants and that the Court grant the following:

A. For an Order certifying the Nationwide Class and the California Class, and appointing Plaintiff and her Counsel to represent each such Class;

B. For equitable relief enjoining Defendants from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of the PII and PHI of Plaintiff and Class Members;

C. For injunctive relief requested by Plaintiff, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and Class Members, including but not limited to an order:

i. prohibiting Defendants from engaging in the wrongful and unlawful acts described herein;

ii. requiring Defendants to protect, including through encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state or local laws;

iii. requiring Defendants to delete, destroy, and purge the personal identifying information of Plaintiff and Class Members unless Defendants can provide to the Court reasonable justification for the retention and use of such information

when weighed against the privacy interests of Plaintiff and Class Members;

iv. requiring Defendants to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the PII and PHI of Plaintiff and Class Members;

v. prohibiting Defendants from maintaining the PII and PHI of Plaintiff and Class Members on a cloud-based database;

vi. requiring Defendants to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

vii. requiring Defendants to engage independent third-party security auditors and internal personnel to run automated security monitoring;

viii. requiring Defendants to audit, test, and train its security personnel regarding any new or modified procedures;

ix. requiring Defendants to segment data by, among other things, creating firewalls and access controls so that if one area of Defendants' network is compromised, hackers cannot gain access to other portions of Defendants' systems;

x. requiring Defendants to conduct regular database scanning and securing checks;

xi. requiring Defendants to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees'

respective responsibilities with handling personal identifying information, as well as protecting the personal identifying information of Plaintiff and Class Members;

xii. requiring Defendants to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

xiii. requiring Defendants to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendants' policies, programs, and systems for protecting personal identifying information;

xiv. requiring Defendants to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendants' information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

xv. requiring Defendants to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves;

xvi. requiring Defendants to implement logging and monitoring programs sufficient to track traffic to and from Defendants' servers; and for a period of 10 years,

appointing a qualified and independent third party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendants' compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment;

D. For an award of damages, including actual, nominal, statutory, and consequential damages, as allowed by law in an amount to be determined;

E. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;

F. For prejudgment interest on all amounts awarded; and

G. Such other and further relief as this Court may deem just and proper.

**DEMAND FOR JURY TRIAL**

Plaintiff hereby demands that this matter be tried before a jury.

Date: June 2, 2021

Respectfully submitted,

*/s/ Joe Kendall*

JOE KENDALL
Texas Bar No. 11260700
**KENDALL LAW GROUP, PLLC**
3811 Turtle Creek Blvd., Suite 1450
Dallas, Texas 75219
214-744-3000 / 214-744-3015 (Facsimile)
jkendall@kendalllawgroup.com

M. ANDERSON BERRY (262879)
(*Pro Hac Vice* application forthcoming)
**CLAYEO C. ARNOLD,**
**A PROFESSIONAL LAW CORP.**
865 Howe Avenue
Sacramento, CA 95825
Telephone: (916) 777-7777
Facsimile: (916) 924-1829
aberry@justice4you.com

RACHELE R. BYRD (190634)
MARISA C. LIVESAY (223247)
BRITTANY N. DEJONG (258766)
**WOLF HALDENSTEIN ADLER FREEMAN & HERZ LLP**
750 B Street, Suite 1820
San Diego, CA 92101
Telephone: 619/239-4599
Facsimile: 619/234-4599
byrd@whafh.com
livesay@whafh.com
dejong@whafh.com

*Attorneys for Plaintiff and the Putative Classes*